RECEIVED
CENTRAL FAX CENTER
MAY 14 2008

PATENT

Docket No.: 200309083-1
App. Ser. No.: 10/679,111

IN THE SPECIFICATION

Please replace the paragraph on lines 5-18, page 7 with the following paragraph:

FIG. 3 is a flowchart of a method 300 according to the present invention for downloading an unknown or unrequested file wherein file server 204 is untrusted and offers a file to PDA 202 at step 302 without making any declaration as to what the file may contain. PDA 202 downloads the file at step 304 and calculates the MD5 checksum at step 306. PDA 202 then contacts trusted directory server 206 at step 308. Upon verification of the checksum by directory server 206 at step 310, PDA 202 retrieves a human readable description from directory server 206 at step 312. The human readable description may be text such as a file or movie name or may some other unique or descriptive identifier. PDA 202 then notifies the user at step 314 that new content has been downloaded and is available for use. In an implementation, usage of the downloaded content is provided by a decryption key that is obtained through payment server 206 upon verification of the checksum at step 310. A link to such key could be provided in the downloaded file or in the returned result from directory server 206. Note that where directory server 206 cannot verify the checksum, the process terminates at step 316 by aborting and deleting the downloaded file from PDA 202.

Please replace the paragraph in lines 4-13, page 10 with the following paragraph:

At step 602, PDA 202 locates an access point. Then at step 604, PDA 202 requests the file MD5ofFile.media. When the request is received, file server 204 locates the appropriate file to be transferred at step 606, that is the file whose MD5 checksum is MD5ofFile. Moreover, file server 204 chooses an appropriate key, K, at step 608. Because hotspot to hotspot communication is not presumed, method 600 provides for the transfer of the key, K,

PAGE 8/22 * RCVD AT 5/14/2008 10:13:42 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-5/21 * DNIS:2738300 * CSID:703 221 5698 * DURATION (mm-ss):06-16

between hotspots without the need for back end communication. In an implementation, PDA 202 itself transfers an encrypted version of the key, K, between hotspots. To do this, each hotspot can have a public/private (e.g., K_{pub}, K_{priv}, respectively) that is distributed to each hotspot. In an implementation, such key pairs may remain constant, however, in yet another implementation, such key pairs may be changed periodically.

Please replace the two paragraphs in the last three lines of page 10 through line 22 of page 11 with the following two paragraphs:

Shown in FIG. 7 is a flowchart for a method 700 by which PDA 202 continues to download a previously partially downloaded file upon identifying a new access point. PDA 202 can be configured to continually search for available access points such that at step 702, PDA 202 locates an access point. Here, the general case can be assumed where the located access point in method 700 is different from the access point of 600. Accordingly, the associated file server 204 can also be assumed to be different. Because PDA 202 already has part of a desired file, it requests continuation of such file, for example, MD5ofFile.media, at step 704. Recall that MD5ofFile.media is encrypted with key, K, but file server 204 associated with the present access point does not have such key, K. PDA 202, however, does have such information in the form of the encrypted file MD5ofFile.key. Thus, at step 706, PDA 202 transmits MD5ofFile.key to file server 204. With such transmitted information, file server 204 is then able to recover the key, K, as well as the MD5 checksum using its private key at step 708. File server 204 then confirms that the recovered key, K, actually corresponds to the desired file, MD5ofFile.media, at step 710 by matching the MD5 checksums. If the correspondence is not confirmed method 700 terminates at step 720. If the correspondence is

PAGE 9/22 * RCVD AT 5/14/2008 10:13:42 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-5/21 * DNIS:2738300 * CSID:703 221 5698 * DURATION (mm-ss):06-16

confirmed, file server 204 can then encrypt the requested media file at step 712 and proceed to transmit at step 714 the remainder of the desired file in an encrypted form. PDA 202 then receives the desired file at step ~~714~~ 716.

In a continuous manner, PDA 202 detects whether the desired file transfer is interrupted at step ~~716~~ 718. Interruptions in file transfer can occur for many reasons, including loss of wireless connection, loss of power to PDA 202, loss of power to file server 204, memory errors, etc. Where an interruption occurs, method 700 can be reinitiated at step 702. That is, PDA 202 will look for an access point from which it can receive the remaining portion of the desired file. Where no interruption occurs, file transfer continues until the complete file is transferred and method 700 terminates at step ~~718~~ 720.

No new matter has been added.

PAGE 10/22 * RCVD AT 5/14/2008 10:13:42 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-5/21 * DNIS:2738300 * CSID:703 221 5698 * DURATION (mm-ss):06-16